

ImmoBill

Sicherheitskonzept — Technische und organisatorische Maßnahmen

Stand: August 2026 · TNF Consulting & Development GmbH, Südbrookmerland

ImmoBill verarbeitet Abrechnungs-, Mieter- und Zahlungsdaten — Daten, die Vertrauen verlangen. Dieses Dokument beschreibt, mit welchen technischen und organisatorischen Maßnahmen ImmoBill diese Daten schützt. Es richtet sich an Kunden, deren Steuerberater und Datenschutzbeauftragte.

1. Betrieb und Hosting

- **Hosting in Deutschland:** Alle Systeme laufen auf Servern in einem deutschen Rechenzentrum (Strato AG, Berlin). Es findet keine Übermittlung von Anwendungsdaten in Drittländer statt.
- **Getrennte Instanzen:** Jeder Kunde erhält eine eigene Installation mit eigener Datenbank und eigenen Zugangsdaten. Eine Vermischung von Daten unterschiedlicher Kunden ist technisch ausgeschlossen; Demonstrationsumgebungen enthalten ausschließlich erfundene Daten.
- **Gepflegte Systeme:** Betriebssystem und Laufzeitumgebung werden aktuell gehalten; sicherheitsrelevante Updates werden automatisch eingespielt. Eine Firewall beschränkt den Zugriff auf die notwendigen Dienste, die Datenbank ist von außen nicht erreichbar.

2. Verschlüsselung

- **Transportverschlüsselung:** Sämtliche Verbindungen laufen ausschließlich über HTTPS mit modernen TLS-Verfahren (TLS 1.2/1.3); veraltete Protokolle sind deaktiviert. Die Zertifikate werden automatisch erneuert, HSTS erzwingt die verschlüsselte Verbindung dauerhaft.
- **Geheimnisse verschlüsselt gespeichert:** Hinterlegte Zugangsdaten zu Drittdiensten (z. B. Bankabruf, E-Mail-Versand) werden mit moderner Kryptografie (libsodium) verschlüsselt abgelegt; die Schlüssel liegen außerhalb des Web-Bereichs und werden nach Erstellung nie wieder im Klartext angezeigt.
- **Passwörter:** Benutzerpasswörter werden ausschließlich als starke Einweg-Hashes (bcrypt) gespeichert — sie sind auch für Administratoren nicht einsehbar.

3. Zugriffsschutz

- **Zwei-Faktor-Anmeldung (2FA):** Anmeldung mit Einmalcodes nach Industriestandard (TOTP, RFC 6238) über gängige Authenticator-Apps; für Administratoren und Sachbearbeiter verpflichtend. Einmalige Backup-Codes sichern den Zugang bei Geräteverlust ab; Anmeldungen von unbekannten Geräten lösen eine Benachrichtigung aus.
- **Schutz vor Angriffsversuchen:** Fehlgeschlagene Anmeldeversuche werden begrenzt und mit ansteigenden Wartezeiten belegt; auffällige Zugriffsmuster werden serverseitig erkannt und blockiert. Anmeldeereignisse werden protokolliert, die letzte Anmeldung wird dem Benutzer angezeigt.

- **Rollen- und Rechemodell:** Jeder Benutzer sieht nur, was seine Rolle erlaubt — vom Administrator über Sachbearbeiter bis zum Mieterzugang, der ausschließlich die eigenen Verbräuche und Abrechnungen anzeigt. Die Rechteprüfung erfolgt serverseitig auf jeder Seite.
- **Sitzungsschutz:** Sitzungen sind gegen Übernahme gehärtet (sichere Cookies, Erneuerung bei Anmeldung) und enden nach längerer Inaktivität automatisch.

4. Datensicherung

- **Tägliche Sicherung:** Datenbanken, Anwendung und Dokumente werden jede Nacht automatisch gesichert.
- **Verschlüsselt außer Haus:** Zusätzlich wird jede Sicherung einzeln stark verschlüsselt (AES-256) und an einen räumlich getrennten Speicherort übertragen. Die Entschlüsselung ist nur mit Schlüsseln möglich, die getrennt und offline verwahrt werden.
- **Getestete Wiederherstellung:** Die Wiederherstellung aus der Sicherung wird nicht nur vorgehalten, sondern tatsächlich geprobt und dokumentiert — inklusive Nachweis, dass wiederhergestellte Daten bit-genau dem Original entsprechen.

5. Sichere Software-Entwicklung

- **Schutz vor gängigen Angriffsklassen:** Durchgängige Absicherung gegen Formularmissbrauch (CSRF-Token), Datenbankangriffe (ausschließlich parametrisierte Abfragen) und Skript-Einschleusung (konsequente Ausgabekodierung, restriktive Content-Security-Policy und weitere Schutz-Header).
- **Regelmäßige Überprüfung:** Die Anwendung wird wiederkehrend einem systematischen Sicherheits-Audit unterzogen; Befunde werden priorisiert und nachweislich behoben.
- **Qualitätssicherung:** Jede Änderung durchläuft eine Testumgebung und automatische Regressionsprüfungen, die die Unversehrtheit bestehender Abrechnungen byte-genau nachweisen, bevor sie produktiv geht.

6. Datenschutz

- **DSGVO:** Die Verarbeitung erfolgt nach den Grundsätzen der Datenminimierung und Zweckbindung; Mieter sehen im Portal ausschließlich die eigenen Daten. Verantwortlicher Betreiber ist die TNF Consulting & Development GmbH.
- **Auftragsverarbeitung:** Für Kunden, die ImmoBill mit personenbezogenen Daten ihrer Mieter nutzen, stellen wir auf Anfrage einen Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) bereit.
- **Keine Weitergabe:** Anwendungsdaten werden nicht an Dritte verkauft oder zu Werbezwecken ausgewertet. Anbindungen an Drittdienste (z. B. Dokumentenarchiv, Bank) erfolgen ausschließlich im Auftrag und Interesse des jeweiligen Kunden.